IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No. 15-CIV-1315
	)	
v.	)	
	)	
ANDREY GHINKUL a/k/a Andrei Ghincul a/k/a "smilex,"	)	
MAKSIM VIKTOROVICH YAKUBETS a/k/a "aqua,"	)	
IGOR TURASHEV a/k/a "nintutu,"	)	
MAKSIM MAZILOV a/k/a "caramba," and,	)	
ANDREY SHKOLOVOY a/k/a "caramba,"	)	
Defendants.	)	

UNITED STATES' MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

Plaintiff, the United States of America, by and through its attorneys, David J. Hickton, United States Attorney for the Western District of Pennsylvania, Leslie R. Caldwell, Assistant Attorney General, Michael A. Comber, Assistant United States Attorney, and Richard D. Green, Senior Trial Attorney, pursuant to 18 U.S.C. §§ 1345, 2521, and Federal Rule of Civil Procedure 65, hereby seeks an *ex parte* temporary restraining order commanding the defendants to halt a massive fraud and wiretapping scheme that is harming consumers, financial institutions, and other businesses in the United States and around the world.

I. OVERVIEW

The defendants in this case are responsible for the infection of a vast number of unsuspecting victims' computers worldwide with malicious software ("malware"): Bugat/Dridex. Bugat/Dridex is a credential harvester that intercepts banking and other online credentials from infected computers and enlists those computers into a "botnet" – a network of infected computers controlled by the defendants. Bugat/Dridex has infected in excess of 100,000 computers in the United States and many more around the world and have generated direct and indirect losses to consumers and businesses that exceed $10 million domestically and likely in excess of $25 million worldwide.

In this action, the United States seeks injunctive relief commanding the defendants to stop using Bugat/Dridex to defraud and wiretap American citizens and businesses. To give effect to this prohibition, the United States seeks permission to employ a series of technical measures designed to disrupt the defendants' malware and free victims from its grasp. Specifically, the United States seeks an Order: (1) authorizing the United States to establish computer infrastructure to gain control of the Bugat/Dridex infected computers; and, (2) directing six companies and organizations listed in Appendix A to redirect inbound internet traffic from six identified super-peers to Government computers.

In addition to the civil relief sought above, the Government has also applied for a Pen Register/Trap and Trace Order that would authorize the collection of the dialing, routing, addressing, and signaling information of communications sent by the computers infected with the Bugat/Dridex malware to the substitute servers and other computer infrastructure established pursuant to the TRO sought by the Government. This information would be disseminated to the

Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), Dell SecureWorks and the ShadowServer Foundation that would facilitate the notification of Bugat/Dridex victims and provide instruction on how to remove these infections from their computers.[1]

This action is the latest in a string of cases brought by public and private sector entities to combat malicious software, and it is very similar to the successful Coreflood botnet disruption, which was initiated in the District of Connecticut in April 2011 ("Coreflood") and the successful botnet mitigation effort in the GameOver Zeus ("GOZ") case here in this District. *See United States v. John Doe 1 et al.* No. 3:11-CV-00561 (D. Conn., filed Apr. 11, 2011) (Coreflood), *United States v. Bogachev*, No. 2:14-CV-0685 (W.D. Pa., filed May 26, 2014) (GOZ). Coreflood and GOZ, like Bugat/Dridex, were botnets used by criminals to intercept financial information, including login credentials, and to execute fraudulent transactions. To disable Coreflood and GOZ, the United States used the same authorities invoked here to deny the operators of Coreflood and GOZ access to the infrastructure necessary to control the botnet. In both Coreflood and GOZ, the Government also received judicial authorization to establish a substitute server to replace the command and control infrastructure operated by the Coreflood and GOZ defendants. These actions successfully crippled the botnet and disabled the criminal enterprise.[2]

---

[1] US-CERT is part of the Department of Homeland Security, and leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. *See* http://www.us-cert.gov/about-us. Dell SecureWorks provides Managed Security Services and is a frequent partner of the FBI. The ShadowServer Foundation is a non-profit security research organization in the Netherlands that frequently hosts servers used in botnet remediation and has strong relationships with U.S. Internet Service Providers (ISPs).

[2] *See* Riva Richmond, "U.S. Dismantles Large Network of PCs Infected by Criminals," N.Y. Times, Apr. 15, 2011, http://query.nytimes.com/gst/fullpage.html?res=9E0DEFD8123EF936A25757C0A9679D8B63; Press Release, Department of Justice, "Department of Justice Takes Action to Disable International Botnet," (Apr. 13, 2011),

In the years since Coreflood, the Microsoft Corporation has brought a number of civil actions against botnet operators. *See* Microsoft civil cases cited *infra* at Section VI(B). In each of these cases, Microsoft has been awarded injunctive relief – similar to the relief sought here – designed to disrupt the criminals' control over the botnet and liberate the infected computers.

The criminal enterprise responsible for Bugat/Dridex has caused significant injury in this District, in the United States, and around the world. To disrupt this criminal enterprise, and to protect American citizens and businesses from falling victim to Bugat/Dridex, the United States respectfully requests that this Court enter the proposed temporary restraining order ("TRO") and order the defendants to show cause why a preliminary injunction should not be granted.

II. BACKGROUND ON BUGAT/DRIDEX

A. Overview

Bugat/Dridex is a multifunctional malware package that is designed to steal banking credentials from infected computers to facilitate the theft of money from victims' bank accounts. *See* Declaration of Special Agent Brian Stevens ("Stevens Decl.") at ¶8. Once a computer is infected with Bugat/Dridex, it becomes an infected computer or "bot," which joins a vast network of infected computers that are controlled and operated by the defendants. *Id.* at ¶7. The Bugat/Dridex malware has been in use since late 2009, initially known as Bugat. *Id.* at ¶8. As the individuals behind the development of Bugat made improvements to the malware and added

---

http://www.justice.gov/opa/pr/2011/April/11-crm-466.html.

See also Matt Apuzzo, "Secret Global Strike Kills 2 Malicious Web Viruses," N.Y. Times, June 2, 2014, http://www.nytimes.com/2014/06/03/world/europe/battling-destructive-computer-viruses-agents-seize-networks-used-by-hackers.html?_r=0; pRelease, Department of Justice, "U.S. Leads Multi-National Action Against 'Gameover Zeus' Botnet and 'Cryptolocker' Ransomware, Charges Botnet Administrator," (June 2, 2014), http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

functionality, the name of the malware changed to Cridex and then Dridex. *Id.* at ¶8. However each version of the malware is based on the same original Bugat source code. *Id.* at ¶8. For this reason, the Bugat family of malware is herein referred to as Bugat/Dridex.

It is estimated that Bugat/Dridex has infected hundreds of thousands of computers worldwide. *Id.* at ¶4. Approximately ten distinct Bugat/Dridex sub-botnets have been observed operating since 2014, and at least one of these sub-botnets has primarily targeted financial institutions located in the United States (known as EB120). *Id.* at ¶17. Security researchers have determined that EB120, during May 2015, was comprised of over 100,000 active bots. *Id.* at ¶17.

As stated above, the principal purpose of Bugat/Dridex is to capture banking credentials from infected computers. *Id.* at ¶5. The defendants then use those stolen credentials to execute unauthorized electronic fund transfers or wire transfers to accounts controlled by the Bugat/Dridex organization. *Id.* at ¶5. Losses attributable to Bugat/Dridex are believed to exceed $25 million. *Id.* at ¶4.

Prior to November 2014, the defendants used a botnet architecture that employed a linear communication channel. *Id.* at ¶18. This architecture provided a communications channel through which a multi-layered command and control (C&C) structure of computers were used to issue instructions directly to each bot. *Id.* at ¶18. Such an architecture is simple to operate but is more vulnerable to disruption and seizure by authorities. *Id.* at ¶19. The defendants changed the control architecture in November 2014 to add peer-to-peer (P2P) functionality to make the botnet infrastructure more resistant to countermeasures by law enforcement. *Id.* at ¶20. This current architecture does not rely on single-line communication between C&C servers and the bots, but

rather allows the bots ("peers") to communicate with super-peers and exchange lists ("peer lists") of other peers with which they can communicate.[3] *Id.* at ¶20. To ensure that this list remains active, the peers regularly request new updated bot routing information from "super-peers" on the network. *Id.* at ¶20. The super-peers get the most updated information directly from the C&C servers that are controlled by the defendants. *Id.* at ¶20. Upon receiving the new routing information from the super-peers, the bots update their lists of peers accordingly. *Id.* at ¶20. In this way, the super-peers serve as relay points for commands coming from the Bugat/Dridex operators and for encrypted data stolen from victim computers to be sent to the perpetrators. *Id.* at ¶20.

Before the upgrade, bots were only able to get updates and commands via the centralized C&C servers. *Id.* at ¶21. The switch to P2P functionality made Bugat/Dridex a more decentralized network, allowing for a more diffused dissemination of updates and commands to the bots, and therefore more resistant to take down measures by law enforcement. *Id.* at ¶21.

B. Bugat/Dridex is Used to Wiretap Victims and to Facilitate the Theft of Funds

Once a computer is part of one of the Bugat/Dridex botnets, the defendants accomplish the theft of confidential credentials to access victim accounts at financial institutions, and ultimately stealing the funds in those accounts, by using the functionality of the Bugat/Dridex malware which includes keystroke logging and web injects. *Id.* at ¶5. Keystroke logging is the action of recording, or "logging," the keys struck on a keyboard. *Id.* at ¶5. This action is usually done surreptitiously by a computer program (e.g., keylogger) to capture the keys typed on a

[3] The lists maintained by the peers contain routing information that includes IP addresses and port numbers of other peers in the botnet. *Id.* at ¶20.

computer without the typist's knowledge. *Id.* at ¶5. Malware that uses keystroke logging often will provide the captured keystrokes to those who caused the malware to be installed or to a place designated by them. *Id.* at ¶5. Through keystroke logging, computer intruders are able to obtain online banking credentials as soon as the user of the infected computer logs into their online bank account. *Id.* at ¶5.

Web injects introduce, or "inject," malicious computer code into a victim's web browser while the victim browses the Internet and "hijacks" the victim's Internet session. *Id.* at ¶6. Different injects are used for different purposes. *Id.* at ¶6. Some web injects are used to display false online banking pages into the victim's web browser to trick the victim into entering online banking information, which is then captured by the individual employing the web inject. *Id.* at ¶6.

III. THE DEFENDANTS

A multi-year FBI investigation has revealed that the defendants, who are leaders of a tightly knit group of cybercriminals based primarily in Russia and Moldova, are responsible for Bugat/Dridex. *Id.* at ¶24. The defendants have deliberately targeted their malicious software at U.S. individuals and companies. *Id.* at ¶24. Although the full scope of harm caused by the defendants is impossible to calculate, the best evidence available suggests that Bugat/Dridex has resulted in losses to U.S. businesses and individuals of more than $10 million with the true number possibly many times higher. *Id.* at ¶24.

The defendants have gone to great lengths to conceal their identities and hide from law enforcement. *Id.* at ¶25. The investigation by the FBI includes review of the defendants' internet chat logs, interviews of victims and industry experts, the establishment of threat specific

industry working groups, search warrants, open source research, requests to foreign governments pursuant to Mutual Legal Assistance Treaties and real time attack monitoring. *Id.* at ¶25. This investigation has revealed that, among other tactics, the individuals running Bugat/Dridex use false identities and online monikers, anonymous internet-based payment systems, and an extensive network of money mules to launder the funds stolen during their high tech bank robberies. *Id.* at ¶25. Despite these tactics, as described below, the FBI has identified a small group of individuals at the very top of the criminal gang responsible for Bugat/Dridex. *Id.* at ¶25. These individuals are described below.

A. Andrey Ghinkul

One of these individuals identified as a leader of this criminal gang is Andrey Ghinkul of Chisinau, Moldova. *Id.* at ¶25. On or about September 18, 2014, Internet security researchers provided the FBI with various screenshots from within Bugat/Dridex administrative portals, which had been updated on or about September 18, 2014.[4] *Id.* at ¶26. One of the pages within these portals listed the account numbers and account names of various Bugat/Dridex users. *Id.* at ¶26.

Through these screenshots and from other information obtained in this investigation, the FBI learned that "smilex" was the online nickname of one of the central figures involved in the Bugat/Dridex conspiracy. *Id.* at ¶27. Additionally, during the course of its investigation, the FBI became aware that the Bugat/Dridex malware group was utilizing a server that was assigned IP address Redacted PII.113. *Id.* at ¶27. Internet security researchers provided the FBI with

[4] Administrative portals are web applications which allow criminals to manage the day-to-day operations of their botnets. *Id.* at ¶23.

information that this server contained the "admin control panels" used by the Bugat/Dridex group. *Id.* at ¶27. These control panels provided an interface by which the Bugat/Dridex botnet operators could issue commands to infected computers. *Id.* at ¶27.

Pursuant to a federal search warrant issued on February 24, 2015, the FBI performed searches of email accounts, including Redacted PII@gmail.com, which, as explained below, is known to be utilized by Defendant "smilex." *Id.* at ¶28. These searches revealed evidence of the development and distribution of the Bugat/Dridex malware. *Id.* at ¶28.

Within the email account Redacted PII@gmail.com, the FBI discovered an email sent by Redacted PII@gmail.com to himself at Redacted PII@gmail.com, containing a single zip file. *Id.* at ¶29. This zip file contained within it an executable file. *Id.* at ¶29. Further analysis of the executable file by an Internet security researcher revealed that it was a first stage loader for the Bugat/Dridex malware family. *Id.* at ¶29. This loader, known as "Lerspeng," attempts to download Bugat/Dridex malware from a set of hardcoded websites. *Id.* at ¶29. Based on information received by Internet security researchers at one point all of the hardcoded websites hosted Bugat/Dridex downloader executables. *Id.* at ¶29.

Through legal process served on Google, the FBI learned that the email account Redacted PII@gmail.com was listed as the recovery email for the email account Redacted PII@gmail.com. *Id.* at ¶30. Based on this information, it is apparent that the owner of the email account Redacted PII@gmail.com is also the owner of the email account Redacted PII@gmail.com. *Id.* at ¶30.

The FBI obtained a search warrant for the contents of the email account Redacted PII@gmail.com. *Id.* at ¶31. An analysis of the contents of this account revealed ten

emails from the provider responsible for hosting the server at IP address Redacted PII.113, spanning the timeframe June 4, 2014 through March 24, 2015. *Id.* at ¶31. Seven of these emails were responses to problem tickets that the owner of Redacted PII@gmail.com submitted to the hosting provider regarding this server. *Id.* at ¶31. Three of these emails were abuse notifications from the provider, asking that the owner of Redacted PII@gmail.com remove malware that had been reported conducting malicious activity from the server. *Id.* at ¶31. Because a hosting facility will only accept problem tickets from, and will only send abuse reports to, an individual who was listed as an administrative contact, the above information indicates that the owner of the email account Redacted PII@gmail.com was an administrator of the server at IP address Redacted PII.113. *Id.* at ¶31.

Furthermore, an email sent by Redacted PII@gmail.com on July 5, 2012 contains text that approximately translates to English as "Hello, my jabber handle is Redacted PII@jabber.org, contact me there." *Id.* at ¶32. The FBI has reviewed numerous jabber chat messages for the user Redacted PII@jabber.org from November 2011 through July 2014. *Id.* at ¶32. In those chats, smilex indicates that he is having great difficulty causing infections with spam emails and solicits assistance from other criminals in developing spam templates. *Id.* at ¶32. The FBI believes that these emails are part of the work development process as smilex creates spam templates for the purpose of causing Bugat/Dridex infections. *Id.* at ¶32.

Based on the information in the preceding paragraphs, the FBI believes that the individual using the email accounts Redacted PII@gmail.com, Redacted PII@gmail.com and Redacted PII@gmail.com, and who utilized these accounts to discuss the furtherance of distributing Bugat/Dridex malware, is the same individual who used the Jabber account

Redacted PII@jabber.org and the online moniker "smilex." *Id.* at ¶33. Lastly, the evidence above positively links Andrey Ghinkul a/k/a Andrei Ghincul to the use of the online identity "smilex." *Id.* at ¶33.

Pursuant to a complaint and an arrest warrant signed by U.S. Magistrate Judge Robert C. Mitchell of the Western District of Pennsylvania on August 27, 2015 (under seal), a request was forwarded to the Cyprus Ministry of Justice through the United States Department of Justice, Ghinkul was arrested on August 28, 2015 by Cyprian authorities while on vacation at the Meltemi Villas Resort in Pafos, Cyprus. An initial appearance was conducted in Cyprus on August 29, 2015 and Ghinkul was ordered to be held without bond until an extradition hearing scheduled on October 12, 2015.

Ghinkul was indicted in the Western District of Pennsylvania on September 16, 2015 for violations of 18 U.S.C. §§ 371 (Conspiracy), 1030(a)(2) (Unauthorized access to a protected computer), 1030(a)(5)(A) (Damage to a Protected Computer); 1343 (Wire Fraud), 1344 (Bank Fraud); and 1349 (Conspiracy to Commit Fraud), arising from his leadership role in the Bugat/Dridex conspiracy. The indictment and complaint against Ghinkul are currently under seal, but will be unsealed on or about October 13, 2015, if the Court grants the TRO sought by the Government.

In addition to Ghinkul, the FBI has identified three other individuals who are part of the criminal enterprise responsible for Bugat/Dridex. These individuals are Maksim Yakubets, Igor Turashev, and "Caramba," (only identified to date by his/her online moniker), and have also been named as defendants in this action.

B. Maksim Yakubets

As discussed above, the FBI has reviewed numerous jabber chat logs from November 2011 through July 2014 involving Andrey Ghinkul, who used the nickname smilex. *Id.* at ¶34. A number of these chats were with an individual using the moniker, "aqua." *Id.* at ¶34. Based on the content of these Jabber chats[5], Jabber chats between Ghinkul and other criminal actors, as well as information provided by reliable sources, the FBI believes that "aqua" is likely to have sufficient control over the Bugat/Dridex botnet to enable him to comply with a TRO from this Court ordering him to halt the scheme. *Id.* at ¶34. Furthermore, in order to provide the broadest possible notice to the defendants, the FBI believes with a reasonable degree of certainty that "aqua" is a nickname used by Maksim Viktorovich Yakubets who was last known to reside in Russia. *Id.* at ¶34.

C. Igor Turashev

Earlier in the Bugat investigation, a pen register was attained on IP address Redacted PII.140. *Id.* at ¶35. This IP address connected tens of thousands of times to a server hosted in Turkey that was associated with the distribution of Bugat/Dridex. *Id.* at ¶35. Google records indicated that this IP address was also used to access the email address Redacted PII@gmail.com. *Id.* at ¶35. The email address Redacted PII@gmail.com is the registration address for the nickname "nintutu" on a number of online forums dedicated to facilitating criminal activity. *Id.* at ¶35. There are also several references to "nintutu" contained within smilex's jabber chats that suggest "nintutu" serves as aqua's administrator. *Id.* at ¶35. Based on this and other information learned during the course of the investigation, the FBI believes that

[5] "Jabber" is a free instant messaging, or chat, platform.

"nintutu" is likely to have sufficient control over the Bugat/Dridex botnet to enable him to comply with a TRO from this Court ordering him to halt the scheme. *Id.* at ¶35. Furthermore, in order to provide the broadest possible notice to the defendants, the FBI believes with a reasonable degree of certainty that "nintutu" is a nickname used by Igor Turashev who was last known to reside in Russia. *Id.* at ¶35.

D. Maksim Mazilov and Andrey Shkolovoy

As discussed above, on or about September 18, 2014, Internet security researchers provided the FBI with various screenshots from within Bugat/Dridex administrative portals, which had been updated on or about September 18, 2014. *Id.* at ¶25. One of the pages within these portals listed the account numbers and account names of various Bugat/Dridex users, including a user known by the nickname "caramba." *Id.* at ¶36. Furthermore, as discussed above, the FBI has reviewed numerous jabber chat logs from November 2011 through July 2014 involving Andrey Ghinkul, who used the name smilex. *Id.* at ¶36. A number of these chats were with the user believed to be "Caramba." Based on the content of these Jabber chats, Jabber chats between Ghinkul and other criminal actors, as well as information provided by reliable sources, the FBI believes that "caramba" is likely to have sufficient control over the Bugat/Dridex botnet to comply with a TRO from this Court ordering them to halt the scheme. *Id.* at ¶36. Furthermore, in order to provide the broadest possible notice to the defendants, the FBI believes with a reasonable degree of certainty that "caramba" is a nickname shared by two individuals, Maksim Mazilov and Andrey Shkolovoy, who are associates and share the Caramba identity. *Id.* at ¶36.

IV. BUGAT/DRIDEX HAVE HARMED AND ATTEMPTED TO HARM VICTIMS IN THIS DISTRICT

Bugat/Dridex has also caused and attempted to cause significant financial losses to business operating in this District. *Id.* at ¶¶11-16. Bugat/Dridex is programmed to defeat the added safeguards that banks place on corporate bank accounts, including one-time authorization codes. *Id.* at ¶43. Accordingly, the defendants often use Bugat/Dridex to target lucrative corporate bank accounts, especially those belonging to small and mid-sized businesses. *Id.* at ¶43. Although it is impossible to fully quantify the losses that this malicious program has caused, the paragraphs below provide the court with an overview of the injury in this District alone.

- From August 31, 2012 through September 4, 2012, a petroleum company in the Western District of Pennsylvania had more than $3.5 million wired from its bank account. Expert malware analysis of computers from the company show that the computers were infected with Bugat/Dridex malware at a time before the first wire transfer. The fraudulent wire transfers were sent to banks in Eastern Europe and not recovered.

- On December 16, 2011, a school district in the Western District of Pennsylvania learned from their bank that a wire transfer of $999,000 was about to be executed. This unauthorized wire was canceled. Subsequent FBI investigation revealed that a computer at the school district was infected with Bugat/Dridex malware at a time before the attempted transfer of funds. The analysis also revealed that the infection was the result of a spam email received on November 8, 2011.

Id. at ¶¶11-16.

V. THE UNITED STATES IS PREPARED TO DISRUPT THE BUGAT/DRIDEX BOTNETS

The FBI has developed a comprehensive technical plan to disrupt the Bugat/Dridex botnet. A review of the technical disruption effort and subsequent remediation campaign is provided below.

[**REDACTED**]

VI. ARGUMENT

A. Jurisdiction and Venue Are Proper in This Court

Sections 1345 and 2521 of Title 18 authorize the United States to "commence a civil action in any Federal court" to enjoin fraud, and to "initiate a civil action in a district court of the United States" to enjoin illegal interception of communications. As detailed above, and in the Complaint filed herewith, the defendants are engaged in fraud and wiretapping against U.S. citizens and businesses on a massive scale. Accordingly, subject matter jurisdiction is proper in this Court. This Court may also exercise personal jurisdiction over the defendants, who are foreign nationals that have deliberately targeted victims in this District. Venue is proper under 28 U.S.C. § 1391(b)(2), for the reasons discussed below in relation to personal jurisdiction.

1. The Defendants Are Subject to Personal Jurisdiction in This Court Because They Have Defrauded and Engaged in Unauthorized Wiretapping of Victims in this District

At the complaint stage, a *prima facie* case by the plaintiff of personal jurisdiction is sufficient. *Eurofins Pharma US Holdings v. BioAlliance Pharma SA*, 623 F.3d 147, 155 (3d Cir. 2010). For claims arising under federal law, serving a summons or filing a waiver of service establishes personal jurisdiction over a defendant who is subject to the jurisdiction of a court of general jurisdiction in the state where the district court is located. Fed. R. Civ. P. 4(k)(1); *see*

Provident Nat'l Bank v. California Federal Sav. & Loan Ass'n, 819 F.2d 434, 437 (3d Cir.1987) ("A federal district court may assert personal jurisdiction over a nonresident of the state in which the court sits to the extent authorized by the law of that state."). Pennsylvania law provides for jurisdiction "to the fullest extent allowed under the Constitution of the United States" and "based on the most minimum contact with [the] Commonwealth allowed under the Constitution of the United States." 42 Pa. Cons.Stat. Ann. § 5322(b); *see Marten v. Godwin*, 499 F.3d 290, 296 (3d Cir. 2007).

Pursuant to the Pennsylvania long-arm statute, this Court may assert personal jurisdiction if the defendants have sufficient "minimum contacts" with this forum and if subjecting the defendants to the court's jurisdiction comports with "traditional notions of fair play and substantial justice." *International Shoe Co. v. Washington*, 326 U.S. 310, 316-17 (1945); *Pinker v. Roche Holdings Ltd.*, 292 F.3d 361, 368-69 (3d Cir. 2002). Where, as here, the cause of action is related to the defendant's contacts with the forum, it is sufficient if the contacts show "purposeful availment" by the defendant of an opportunity to conduct activity in the forum state. *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985) ("Jurisdiction is proper . . . where the contacts proximately result from actions by the defendant *himself* that create a "substantial connection" with the forum).

The defendants' victims include individuals and businesses within Pennsylvania. The defendants have not only infected computers in Pennsylvania with Bugat/Dridex, but have intentionally caused significant harm, and attempted harm in this Commonwealth through bank account intrusions and the stealing of bank funds as well as attempts to do so. In so doing, the defendants have purposefully directed their conduct at Pennsylvania. Accordingly, the defendants' conduct readily satisfies the "minimum contacts" requirement of due process, and personal jurisdiction is consistent with the Pennsylvania long-arm statute, quoted above.

2. The Court Should Authorize Service of Process by Internet Publication and Delivery to Defendants' Last-Known Addresses

Unless otherwise prohibited by federal law or international agreement, an individual outside the United States may be served "as the court orders." Fed. R. Civ. Pro. 4(f)(3). The method of service selected must be "reasonably calculated, under all circumstances, to apprise interested parties of the pendency of the action" and afford them an opportunity to be heard." *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950).

Here, defendant Ghinkul is currently in custody in Cyprus. The remaining defendants are believed to reside in Russia, but their precise locations are not known. In order to ensure that these defendants are notified of the pendency of this action, the Government purposes to provide notice of this action through a number of methods.

First, the Government will serve the Complaint, Summons, TRO, and related filings ("Court Filings") via a Mutual Legal Assistance Treaty request for delivery upon defendant Ghinkul at his custodial location in Cyprus.

Second, the Government will send the Court Filings via overnight delivery to last known addresses in Russia that the FBI believes, at least at one time, were the addresses used by Yakubets, Turashev, Mazilov, and Shkolovoy.

Third, the Government will provide notice to Mazilov, and Shkolovoy sharing "caramba," Yakubets as "aqua," and Turashev as "nintutu" through electronic messages. Through the course of the FBI's investigation, the Government has uncovered email addresses and Jabber addresses used by these three defendants. The Government will send the Court Filings to these email addresses and Jabber addresses, which should provide these three defendants with notice of this suit.

Fourth, the Government's will post copies of the Court Filings on the websites of the Department of Justice and the FBI (linked to the Department of Justice posting). If the TRO is granted, all press releases issued by the Department of Justice and the FBI with respect to this matter will direct the defendants to the websites where those pleadings can be accessed. Moreover, because the Government's plan to assist victims of Bugat/Dridex includes substantial media engagement, it is likely that the defendants will learn that the Department of Justice and FBI are involved in the disruption of their infrastructure. There is therefore good cause to believe that the defendants will seek additional information by visiting the public Internet sites of the Department of Justice and FBI and will thereby be notified of this action.

The service plan outlined above is very similar to what was proposed and ultimately approved by the courts in both Coreflood and GOZ. As in GOZ, the methods of service proposed above are even more likely to provide notice to the defendants in this suit as compared to the Coreflood defendants because – unlike in Coreflood – the Government knows the true

name of the lead defendant and will serve him at his current location. Moreover, the Government is not aware of any international agreement that prohibits the methods of service proposed above. Accordingly, pursuant to Rule 4(f)(3), the Court should approve the Government's plan for service of process.

B. The Court May Authorize the United States to Implement the Technical Disruption Described Above to Stop the Ongoing Fraud and Unlawful Interception of Communications Perpetrated by the Bugat/Dridex Botnet

As described in more detail above, the TRO sought by the Government would direct six companies and organizations to redirect inbound traffic to IP addresses used to maintain communications between Bugat/Dridex infected computers with the defendant's command and control architecture and send that traffic to the substitute servers established pursuant to this Court's Order. By ordering this relief, the Court will halt the defendants' use of Bugat/Dridex to defraud and wiretap U.S. citizens and businesses, and will preserve the status quo while private-sector partners identify and notify victims and assist in removing the defendants' malicious software from their computers.

District Courts generally have broad discretion in deciding whether to grant injunctive relief. *See General Instrument Corp. of Delaware v. Nu-Tek Elecs. & Mfg., Inc.*, 197 F.3d 83, 90 (3d Cir. 1999). As courts of equity, District Courts "'may, and frequently do, go much farther both to give and withhold relief in furtherance of the public interest than they are accustomed to go when only private interests are involved.' . . . This is especially the case where the public interest in question has been formalized in a statute." *Instant Air Freight Co. v. C.F. Air Freight, Inc.*, 882 F.2d 797, 803 (3d Cir. 1989) (quoting *Virginian Ry. Co. v. System Fed'n No. 40*, 300 U.S. 515, 552 (1937)). In particular, the Third Circuit has noted that injunctive relief is "in the

broadest sense for the discretion of the trial court which is best qualified to form a judgment as to the likelihood of a repetition of the offense." *U.S. v. Article of Drug Designated B-Complex Cholinos Capsules*, 362 F.2d 923, 928 (3d Cir. 1966).

Sections 1345 and 2521 of Title 18 enhance the Court's traditional powers at equity by allowing the Court to promptly enjoin ongoing fraudulent or unauthorized interception upon a suit by the Government. These statutes confer broad authorization for courts to enter restraining orders "at any time," or to "take such other action, as is warranted to prevent a continuing and substantial injury." 18 U.S.C. §§ 1354(b), 2521. In particular, Section 1345

> authorizes broad injunctive relief . . . for any violation of chapter 63 [and is] a powerful weapon in the government's anti-fraud arsenal. In addition to authorizing injunctive relief . . . the statute empowers courts to enter restraining orders, prohibitions, and "take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of person for whose protection the action is brought." . . . As a result, civil suits under § 1345 are often used to preserve the status quo during a lengthy parallel criminal probe.

United States v. Payment Processing Ctr., 435 F. Supp.2d 462, 464 (E.D. Pa. 2006); *see also id.* at 466 (citing *United States v. Cen-Card Agency/C.C.A.C.*, No. 88-5764, 1989 WL 30653 (3d Cir. March 23, 1989) (discussing past use of Section 1345 to stop fraud)). Indeed, Congress enacted Section 1345 specifically "to allow the Attorney General to put a speedy end to a fraud scheme by seeking an injunction in federal District Court whenever he determines he has received sufficient evidence of a violation of Chapter 63 to initiate such an action," and intended the District Court "to grant such action as is warranted to prevent a continuing and substantial injury to the class of persons designed to be protected by the criminal statute." S. Rep. No. 98-225, at 402 (1984). The use of similar statutory language in Section 2521, enacted after Section 1345, suggests a similar Congressional intent to permit the Attorney General to "put a speedy end" to

ongoing unlawful interceptions. *See also* S. Rep. No. 99-541, at 34 (1986). The Government seeks the relief set forth herein for precisely those purposes.

Civil injunctive relief, such as that sought in this application, has been used in several Districts to accomplish large-scale disruptions of widespread computer hacking. In some cases, the United States Government has been the plaintiff, and in others, a private party has sought the injunctions. In all cases, injunctions have enabled the plaintiffs to halt hackers' schemes without infringing upon the privacy or property interests of victims or other parties.

For example, in Coreflood, the United States District Court for the District of Connecticut, pursuant to 18 U.S.C. §§ 1345 and 2521, enjoined a series of John Doe defendants from running the Coreflood botnet software.[6] The court based its ruling on the Government's showing that the John Doe defendants were using Coreflood to commit wire and bank fraud and to engage in unauthorized electronic surveillance, that the defendants' conduct was causing a continuing and substantial injury, and that the requested restraining order would prevent or ameliorate that injury. The Coreflood order authorized the FBI to establish a substitute server to replace the botnet command and control server formerly run by the defendants and compelled the Domain Registries and Registrars responsible for the domain names used by the Coreflood malware to redirect to the substitute server all traffic intended for the Coreflood domains.

[6] 18 U.S.C. § 1345, combined with the court's inherent equitable authority, was also the basis upon which the U.S. District Court for the Eastern District of Missouri entered a temporary restraining order enjoining individuals from transferring domain names and ordering registrars and registries not to change registration for specified domains, and subsequently entered a permanent injunction with the additional requirement that the registration of defendants' domain names be transferred to non-U.S. registrars. *United States v. Betonsports PLC*. No. 4:06CV01064, 2006 WL 3257797, at *8-9 (E.D. Mo. Nov. 9, 2006); Temporary Restraining Order, *United States v. Betonsports PLC*, No. 4:06CV01064 (E.D. Mo. July 17, 2006).

More recently, in the GameOver Zeus (GOZ) case, *United States v. Bogachev*, No. 2:14-CV-0685 (W.D. Pa., filed May 26, 2014), here in the Western District of Pennsylvania, this District Court enjoined defendants from running the GOZ and Cryptolocker malware again pursuant to 18 U.S.C. §§ 1345 and 2521. The court based its ruling on the Government's showing that the defendants were using GOZ and Cryptolocker to commit wire and bank fraud and to engage in unauthorized electronic surveillance, that the defendants' conduct was causing a continuing and substantial injury, and that the requested restraining order would prevent or ameliorate that injury. The GOZ order, as was the case in Coreflood, authorized the FBI to establish a substitute server to replace the botnet command and control server formerly run by the defendants and compelled the Domain Registries and Registrars responsible for the domain names used by the GOZ and Cryptolocker malware to redirect to the substitute server all traffic intended for the GOZ and Cryptolocker domains.

Similarly, in Microsoft's action against the ZeroAccess botnet, the Western District of Texas entered an injunction granting very similar relief to the relief sought here. Specifically, the Court ordered Domain Registries to redirect traffic from ZeroAccess domains to a substitute command and control server, and ordered 45 U.S. ISPs to block their customers from connecting to a series of malicious IP addresses specified by Microsoft. *See Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, *ZeroAccess*, *supra*. Microsoft has obtained similar injunctions in a number of courts throughout the country. *See, e.g.*, *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, *Microsoft Corp. v. Patti et al.*, 1:11 CV 01017 (Sep. 22, 2011); Second Amended *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary

Injunction, *Microsoft Corp. v. John Does 1-11 Controlling a Computer Botnet Thereby Injuring Microsoft and its Customers*, 2:11 CV 00222 (Mar. 9, 2011); *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, *Microsoft Corp. v. John Does 1-27, Controlling a Computer Botnet Thereby Injuring Microsoft and its Customers*, No. 1:10 CV 156 (E.D.Va. Feb. 22, 2010).

1. Statutory Framework

Section 1345 of Title 18 authorizes the Attorney General to commence a civil action for injunctive relief whenever "a person is violating or about to violate this chapter." 18 U.S.C. § 1345(a)(1)(A). The referenced chapter of Title 18 includes Sections 1343 (Fraud by wire, radio, or television) and 1344 (Bank fraud), statutes the defendants are fragrantly violating through the use of Bugat/Dridex. Section 1345 further provides that a "permanent or temporary injunction or restraining order shall be granted," and that the "court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought." 18 U.S.C. § 1345(a)(3), (b).

Section 2521 of Title 18 similarly authorizes injunctions against illegal interception of communications in violation of 18 U.S.C. § 2511:

> Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United

States or to any person or class of persons for whose protection the action is brought.

Because Bugat/Dridex harvests user credentials by illegally intercepting the communications between infected computers and Internet websites, Section 2521 also empowers the Government to seek the injunctive relief proposed in this action.

2. The United States May Obtain an Injunction Pursuant to 18 U.S.C. § 1345 and 18 U.S.C. § 2521 Without Demonstrating the Traditional Prerequisites for Injunctive Relief

Where, as here, the United States seeks an injunction pursuant to federal statutes enacted to protect the public interest that provide for injunctive relief, the Court is authorized to issue the injunction if the statutory conditions are satisfied. *See United States v. Nutrition Serv., Inc.*, 227 F. Supp. 375, 388–89 (W.D. Pa. 1964), *aff'd* 347 F.2d 233 (3d Cir. 1965) ("There is sufficient showing [for an injunction], whereas here, the Government presents evidence of violations of the provisions of a statute enacted for the protection of the public. . . . Nor is it necessary to demonstrate the precise way in which violations of the law might result in injury to the public interest. It is sufficient to show only that the threatened act is within the declared prohibition of Congress."); *United States v. Sene X Eleemosynary Corp.*, 479 F. Supp. 970, 980 (S.D. Fla. 1979) ("Where an injunction is authorized by statute, it is proper to issue such an order to restrain violations of the law if the statutory conditions are satisfied."). The United States thus is not required to demonstrate the traditional prerequisites for a TRO or preliminary injunction, such as irreparable harm or sufficient public interest. *See United States v. Livdahl*, 356 F.Supp.2d 1289, 1290-91 (S.D. Fla. 2005); *Sene X Eleemosynary Corp.*, 479 F. Supp. at 980–81 ("It is sufficient to show only that the threatened act is within the declared prohibition of Congress."); *Nutrition Serv., Inc.*, 227 F. Supp. at 388–89; *see also Government of the Virgin Islands v. Virgin Islands*

Paving, 714 F.2d 283, 286 (3d Cir. 1983) (superseded on other grounds by statute, *see Edwards v. Hovensa*, 497 F.3d 355, 359 (3d Cir. 2007); *United States Postal Service v. Beamish*, 466 F.2d 804, 806 (3d Cir. 1972); *CSX Transp., Inc. v. Tennessee Bd. Of Equalization*, 964 F.2d 548, 551 (6th Cir. 1992).[7]

3. The United States Is Authorized to Obtain Injunctive Relief Under 18 U.S.C. § 1345 and 18 U.S.C. § 2521 Because Defendants Are Committing Bank and Wire Fraud and Are Illegally Intercepting Electronic Communications

As detailed in Special Agent Stevens' Declaration, and summarized above, the defendants are engaged in wire fraud, bank fraud, and illegal interception of communications on a massive scale through the use of Bugat/Dridex. The United States is therefore fully authorized to obtain an injunction under both 18 U.S.C. § 1345 and 18 U.S.C. § 2521.

When, as here, a federal statute empowers the Government to obtain an injunction prohibiting further violations of criminal law, courts are split on whether the United States must show that there is probable cause to believe the defendant is violating or is about to violate any of the enumerated offenses, or must demonstrate such violations by a preponderance of the evidence. *Compare United States v. Luis,* 966 F.Supp.2d 1321, 1326 (S.D. Fla. 2013) (probable cause; collecting cases) and *United States v. Payment Processing Ctr., LLC*, 461 F. Supp. 2d 319, 323 & n.4 (E.D. Pa. 2006) (probable cause) with *United States v. Brown*, 988 F.2d 658, 663 (6th Cir. 1993) (preponderance) and *United States v. Williams*, 476 F.Supp.2d 1368, 1374 (M.D.Fla.2007) (preponderance). This issue has not been decided by the Third Circuit. In any event, given the overwhelming evidence of criminal conduct presented in Special Agent Stevens'

[7] In passing a statute authorizing injunctive relief, Congress implicitly finds that a violation of the law will irreparably harm the public interest. *See Nutrition Serv., Inc.*, 227 F. Supp. at 388–89.

Declaration, the United States easily meets its burden of proof under 18 U.S.C. § 1345 and 18 U.S.C. § 2521 regardless of which evidentiary standard is applied.

a. The Defendants Are Committing Wire Fraud (18 U.S.C. § 1343)

The elements of wire fraud are: (1) a scheme to defraud; (2) use of the wires for the purpose of executing the scheme; and (3) fraudulent intent. *Devon IT, Inc. v. IBM Corp.*, 805 F. Supp. 2d 110, 123 (E.D. Pa. 2011) (citing *United States v. Pharis*, 298 F.3d 228, 234 (3d Cir. 2002)); *see National Sec. Systems, Inc. v. Iola,* 700 F.3d 65, 105 (3d Cir. 2012). The defendants' conduct readily establishes all of these elements. The defendants operate the Bugat/Dridex botnet for the purpose of stealing online credentials and using those credentials to gain unauthorized access to financial accounts. Once these credentials are harvested, the defendants use the credentials to pose as their victims and log into their bank accounts over the Internet. The defendants then initiate fraudulent wire and ACH transfers in order to empty the bank accounts they have compromised.

b. The Defendants are Committing Bank Fraud (18 U.S.C. § 1344)

The elements of bank fraud are: (1) a scheme to defraud a federally insured financial institution; (2) the defendant participated in the scheme by means of false pretenses, representations, or promises that were material; and (3) the defendant acted knowingly. *United States v. Goldblatt*, 813 F.2d 619, 624 (3d Cir. 1987); *McCoy-McMahon v. Godlove*, No. 08-CV-05989, 2011 WL 4820185, at *12 (E.D. Pa. Sept. 30, 2011). The defendants' criminal conduct satisfies each of these elements. First, the defendants use the Bugat/Dridex botnet to conduct fraudulent financial transfers from federally insured banks, as exemplified by the specific Bugat/Dridex attacks described above. Second, the defendants make materially false

representations to both the bank and the victim to perpetrate their fraudulent scheme, both in tricking victims into installing malware and in impersonating victims to conduct the fraudulent transfers. Finally, the defendants act knowingly and intentionally, as demonstrated by their operation of highly sophisticated botnet software to accomplish their fraud.

c. The Defendants are Unlawfully Intercepting Electronic Communications (18 U.S.C. § 2511)

It is a violation of the Wiretap Act to:

> intentionally intercept, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> [or to]
>
> intentionally use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

18 U.S.C. § 2511(1)(a), (d); (4)(a). As described in the Declaration of Special Agent Stevens, Bugat/Dridex is a highly advanced communications interception platform that exists to harvest online credentials by intercepting communications between infected computers and financial websites. Through the use of Bugat/Dridex's web injects, these credentials are harvested in real time as they are transmitted from the victim's computer. Similarly, Bugat/Dridex's feature that allows for keystroke logging also allows for the harvesting of credentials as they are transmitted in real time. This conduct clearly violates 18 U.S.C. § 2511(1)(a) and (d).

4. The Proposed Disruption Is Neither A Fourth Amendment Search nor Seizure and Does Not Require the Issuance of a Warrant

The Government's planned disruption of Bugat/Dridex is neither a search nor a seizure under the Fourth Amendment. Accordingly, this court may authorize the proposed disruption without the issuance of a warrant.

In order to constitute a Fourth Amendment search, the government's actions must either invade an individual's reasonable expectation of privacy, or constitute a physical trespass upon property for the purpose of obtaining information. *See United States v. Jones*, 132 S.Ct. 945, 951 (2012); *Ware v. Donahue*, 950 F.Supp. 2d 738, 744 (D. Del. 2013) (differentiating between a Fourth Amendment search and seizure, and explaining that a "search occurs when an individual's reasonable expectation of privacy is infringed").

Nothing in the planned operation constitutes a Fourth Amendment search. If approved, the only information gathered by the Government during the operation will be dialing, addressing, routing, and signaling information that will be recorded by the Government when infected computers check in at the substitute servers. There is no reasonable expectation of privacy in this information, which will be collected pursuant to a Pen/Trap Order. *See, e.g. United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010) ("no reasonable expectation of privacy exists in an IP address"); *United States v. Forrester*, 512 F.3d 500, 510-12 (9th Cir. 2008) (holding that Government surveillance techniques that reveal non-content information, including the to/from addresses of e-mail messages, the IP addresses of websites visited, and the total amount of data transmitted to or from an account, do not constitute a Fourth Amendment search).

The planned disruption also does not constitute a seizure. A seizure occurs when the Government meaningfully interferes with an individual's possessory interests in property. *Soldal*

v. Cook Cnty., 506 U.S. 56, 61 (1992). Here, the proposed operation would cause no meaningful interference with the victims' possessory interests in their computers, or any other possessory interest. If the Court grants the TRO, computers infected with Bugat/Dridex will be prevented from communicating with computers controlled by the defendants, and will begin exchanging routing information with the substitute servers established by this Court's Order. This transition will be completely transparent to the user, whose computer will perform all authorized functions exactly as it has before. This imperceptible change does not constitute a meaningful interference with the user's possessory interests.

5. *Ex Parte* Relief is Appropriate

The purpose of a temporary restraining order is to preserve the status quo until the Court has an opportunity to pass on the merits of a preliminary injunction. *See Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers Local No. 70*, 415 U.S. 423, 439 (1974); *Garcia v. Yonkers Sch. Dist.*, 561 F.3d 97, 107 (2d Cir. 2009). A District Court may grant a temporary restraining order without notice to defendants if "specific facts in an affidavit or verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition," and the movant "certifies in writing any efforts made to give notice and the reasons why it should not be required." Fed. R. Civ. P. 65(b)(1).

The relief sought herein would preserve the status quo by preventing the defendants from defrauding additional individuals and financial institutions. As discussed herein, the ongoing and aggressive fraud the Government seeks to stop will likely continue to cause irreparable injury and loss until it is halted. Prior notice to the defendants would render futile the

Government's efforts to stop the defendants' ongoing criminal acts. If notified in advance of the Government's intended actions, the defendants could and would take simple, rapid steps to blunt or defeat the Government's planned disruption of the Bugat/Dridex botnet. *See* Stevens Decl. ¶37. Such steps would likely include reestablishing their command and control infrastructure and/or making significant changes to the intermediary communication protocols, which would not take extensive time or effort. *Id.* at ¶37. Bugat/Dridex is a rapidly evolving malware set, and the Defendants are skilled cyber criminals, easily able to change the malware. *Id.* at ¶38. Nearly the entire Bugat/Dridex botnet can be updated within 24 hours. *Id.* at ¶38. The Bugat/Dridex botnet has been updated in this manner previously, including in response to the prior takedown of the GameOver Zeus botnet in 2014. *Id.* at ¶38.

The requested *ex parte* relief is necessary to prevent such evasion of the Government's remedial measures. *See* 18 U.S.C. §§ 1345(b) (the "court shall . . . take such other action as is warrant to prevent a continuing and substantial injury"), 2521 (same); Fed. R. Civ. P. 65(b)(1).

6. A Sealing Order Should be Entered in this Case

As set forth in the Government's request for leave to file under seal, the Government respectfully requests leave to file this memorandum, the Complaint, the proposed TRO, and all associated documents under seal. The Government further requests leave to file redacted versions of these documents at the time they are unsealed in order to protect an ongoing law enforcement investigation in this case and similar law enforcement investigations in the future.

Conclusion

For the foregoing reasons, the Government respectfully requests the Court grant the Temporary Restraining Order requested by the Government.

Respectfully submitted,

DAVID J. HICKTON
United States Attorney

By: /s/ Michael A. Comber
MICHAEL COMBER
Assistant U.S. Attorney
Western District of PA
U.S. Post Office & Courthouse
700 Grant Street, Suite 4000
Pittsburgh, PA 15219
(412) 894-7485 Phone
(412) 644-6995 Fax
PA ID No. 81951
Michael.Comber@usdoj.gov

LESLIE R. CALDWELL
Assistant Attorney General

By: /s/ Richard D. Green
RICHARD D. GREEN
Senior Trial Attorney
Computer Crime and Intellectual Property Section
1301 New York Avenue NW
Washington, DC 20530
(202) 514-1026 Phone
(202) 514-6113 Fax
PA Bar No. 43758
Richard.Green@usdoj.gov